

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
155 NORTH WACKER DRIVE
CHICAGO, ILLINOIS 60606-1720

TEL: (312) 407-0700
FAX: (312) 407-0411
www.skadden.com

FIRM/AFFILIATE OFFICES

BOSTON
HOUSTON
LOS ANGELES
NEW YORK
PALO ALTO
WASHINGTON, D.C.
WILMINGTON

BEIJING
BRUSSELS
FRANKFURT
HONG KONG
LONDON
MUNICH
PARIS
SÃO PAULO
SEOUL
SHANGHAI
SINGAPORE
TOKYO
TORONTO

CONFIDENTIAL

October 5, 2023

Via Email to IDTheft@oag.state.md.us

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Flagstar – Vendor MOVEit Incident

Dear Attorney General:

We write to inform you that Flagstar Bank, N.A. (“Flagstar” or “the Bank”), 5151 Corporate Drive, Troy, Michigan 48098, was notified by Fiserv, a third-party vendor that the Bank uses for payment processing and mobile banking, that it was subject to the security incident involving the MOVEit file transfer system. The incident did not affect Flagstar’s systems.

Between May 27 and 31, an unauthorized party was able to access the vendor’s instance of the MOVEit file transfer system through a zero day vulnerability. The vendor launched a comprehensive investigation, identified individuals affected and notified regulatory bodies as required. After a forensic investigation and manual document review, the vendor determined that unauthorized actors obtained vendor files that included personal information associated with Flagstar customers, such as name, address, Social Security Number/tax ID number, date of birth, and/or financial account number without any password or security code that may have provided access to the account. Flagstar has determined that 1,667 Maryland residents were affected by the incident.

Office of the Attorney General
October 5, 2023
Page 2

The vendor and Flagstar have reported the matter to law enforcement. For the convenience of Maryland's impacted residents, Flagstar has arranged to make credit monitoring and identity repair services available to them at no cost for two years.

The formal notice will be sent to the affected residents via first-class U.S. Mail beginning on October 6, 2023. A copy of the consumer notice template is attached. Please contact me if you have any questions.

Sincerely,

A handwritten signature in blue ink, appearing to read "William E. Ridgway", is positioned above a horizontal line.

William E. Ridgway
Counsel to Flagstar Bank, N.A.
155 N. Wacker Dr.
Chicago, IL 60606
William.Ridgway@skadden.com

Enclosure

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

IMPORTANT INFORMATION, PLEASE REVIEW CAREFULLY

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

What Happened?

We are contacting you regarding an incident that impacted Fiserv, a third-party vendor (“vendor”) Flagstar Bank uses for payment processing and mobile banking purposes, in which some of your personal information was disclosed to an unauthorized party. The incident involved vulnerabilities discovered in MOVEit Transfer, a file transfer software used by our vendor to support services it provides to Flagstar and its related institutions. MOVEit is a commonly used secure Managed File Transfer (MFT) software supporting file transfer activities by thousands of organizations around the world. Importantly, the vulnerability discovered in MOVEit did not involve any of Flagstar Bank’s systems and did not impact our ability to service our customers.

Our vendor promptly launched an investigation into the nature and scope of the MOVEit vulnerability’s impact on its systems and discovered that the unauthorized activity in the MOVEit Transfer environment occurred between May 27 and 31, 2023, which was before the existence of this vulnerability was publicly disclosed. During that time, unauthorized actors obtained our vendor files transferred via MOVEit. These files included Flagstar Bank and related institution customer information, including yours.

What Information Was Involved?

Our vendor conducted a careful review of the contents of the files and on <<b2b_text_2 (Date of Incident)>>, determined that one or more of the files may have contained information including <<b2b_text_3 (your name, impacted data elements)>>.

What We Are Doing.

We wanted to notify you of this incident and to assure you that we take it seriously. Upon learning of this incident, Flagstar took immediate action to ensure that our vendor had launched a comprehensive investigation, identified individuals affected and notified regulatory bodies as required. To help prevent something like this happening again our vendor has, through their service provider, remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider’s guidelines. Our vendor’s service provider also mobilized a technical response team to examine the relevant MOVEit systems and ensure that there were no further vulnerabilities.

What You Can Do.

We have arranged for you to receive a complimentary free identity monitoring service through Kroll for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

For more information on identity theft prevention, including instructions on how to activate your identity monitoring, as well as some additional steps you can take for your protection, please review Attachments A and B that are enclosed with this letter.

Regardless of whether you elect to activate the identity monitoring service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify us or any other of your financial institutions if you suspect any unauthorized activity.

For More Information.

Please be assured that we, along with our vendor, are taking steps to address the incident and to help protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact the dedicated response line at (866) 846-0177, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

<<b2b_text_1 (Data Owner Name)>>

ATTACHMENT A

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ATTACHMENT B

ADDITIONAL STEPS YOU CAN TAKE

To help protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:
Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your

personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; Telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000 (From Outside North Carolina.)

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

* * * * *

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*In Addition, New Mexico Consumers Have the Right to
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

* * * * *

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, Telephone: 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant

to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were 286 Rhode Island residents impacted by this incident.

Dear Attorney General,

We write to update you on a notice that Flagstar Bank, N.A. (“Flagstar” or “the Bank”), 5151 Corporate Drive, Troy, Michigan 48098, submitted on October 5, 2023 regarding the incident related to the zero-day vulnerability of the MOVEit file transfer system affecting Fiserv, a third-party vendor that the Bank uses for payment processing and mobile banking purposes. After it sent out the initial notices, Flagstar identified additional impacted files that were not available to the Bank for review during the initial investigation of the incident. Following a detailed review of the contents of these files, Flagstar determined that an additional 94 Maryland residents were impacted. Please contact me if you have any questions.

Regards,
Branka Cimesa

Branka Cimesa
Associate
Skadden, Arps, Slate, Meagher & Flom LLP
[155 N. Wacker Drive | Chicago | Illinois | 60606-1720](#)
[T: +1.312.407.0671](#) | [M: +1.847.612.2601](#)
branka.cimesa@skadden.com

From: Cimesa, Branka (CHI)
Sent: Thursday, October 5, 2023 4:44 PM
To: 'IDTheft@oag.state.md.us' <IDTheft@oag.state.md.us>
Cc: Ridgway, William (CHI) <William.Ridgway@skadden.com>
Subject: Flagstar - Vendor MOVEit Incident - MD

To Whom it May Concern,

Attached please find a notice of the incident referenced above.

Sincerely,
Branka Cimesa

Branka Cimesa
Associate
Skadden, Arps, Slate, Meagher & Flom LLP
[155 N. Wacker Drive | Chicago | Illinois | 60606-1720](#)
[T: +1.312.407.0671 | M: +1.847.612.2601](#)
branka.cimesa@skadden.com

This email (and any attachments thereto) is intended only for use by the addressee(s) named herein and may contain legally privileged and/or confidential information. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution or copying of this email (and any attachments thereto) is strictly prohibited. If you receive this email in error please immediately notify me at (212) 735-3000 and permanently delete the original email (and any copy of any email) and any printout thereof.

Further information about the firm, a list of the Partners and their professional qualifications will be provided upon request.

=====